

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC971 U.S. PTO
09/862888
05/21/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年10月 6日

願 番 号
Application Number:

特願2000-307822

願 人
Applicant(s):

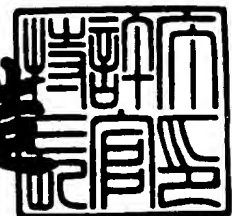
村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月23日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3023002

【書類名】 特許願

【整理番号】 21573

【提出日】 平成12年10月 6日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
H04K 1/00

【発明の名称】 暗号化方法，復号方法，暗号通信方法，暗号通信システム及び記録媒体

【請求項の数】 10

【発明者】

 【住所又は居所】 滋賀県大津市仰木の里東8丁目7-12

 【氏名】 片柳 磨子

【発明者】

 【住所又は居所】 京都府京都市伏見区竹田向代町136番地 村田機械株式会社 本社工場内

 【氏名】 村上 恭通

【発明者】

 【住所又は居所】 大阪府箕面市粟生外院4丁目15番3号

 【氏名】 笠原 正雄

【特許出願人】

 【識別番号】 000006297

 【氏名又は名称】 村田機械株式会社

 【代表者】 村田 純一

【特許出願人】

 【識別番号】 597008636

 【氏名又は名称】 笠原 正雄

【代理人】

 【識別番号】 100078868

 【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法、復号方法、暗号通信方法、暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項 1】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる k 個の成分を有する第 1 ベクトル、 n 個の任意の乱数を成分とする第 2 ベクトル、及び、前記 k 個の成分または前記 n 個の成分の位置を特定する情報を示す h 個の成分を有する第 3 ベクトルを加えた $K (= k + n + h)$ 個の成分を有する第 4 ベクトルと、公開されている第 5 ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項 2】 前記暗号文は、前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第 4 ベクトルにおける前記 h 個の成分の位置は同一である請求項 1 に記載の暗号化方法。

【請求項 3】 前記暗号文は、前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記 k 個の成分に応じて次のブロックでの前記第 4 ベクトルにおける前記 k 個の成分または前記 n 個の成分の位置を決定する請求項 1 に記載の暗号化方法。

【請求項 4】 前記暗号文は、前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる 1 つのブロックと、前記第 3 ベクトルの h 個の成分を平文を分割してなる h 個の成分に置き換えた前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記 k 個または $(k + h)$ 個の成分に応じて次のブロックでの前記第 4 ベクトルにおける $(k + h)$ 個の成分または前記 n 個の成分の位置を決定する請求項 1 に記載の暗号化方法。

【請求項 5】 前記第 5 ベクトルは、1 または複数組の整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて各組毎に K 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_K$ (任意の 2 つの整数 d_i, d_j は互いに素)) に設定された 1 または複数の第 6 ベクトルとを用いて生成する請求項 1 ~ 4 の何れ

かに記載の暗号化方法。

【請求項 6】 前記第 4 ベクトルの各成分と、前記第 6 ベクトルを基にモジュラ変換した前記第 5 ベクトルの各成分とによる積和演算により暗号文を得るようにした請求項 5 に記載の暗号化方法。

【請求項 7】 請求項 1 ～ 6 の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記第 1 ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする復号方法。

【請求項 8】 第 1 のエンティティ側で、請求項 1 ～ 6 の何れかに記載の暗号化方法に従って平文から暗号文を作成して第 2 のエンティティ側へ伝送し、伝送された暗号文を該第 2 のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、平文を分割してなる前記 k 個もしくは $(k + h)$ 個の成分または前記 n 個の成分の位置を前記一方のエンティティ側で任意に決定することを特徴とする暗号通信方法。

【請求項 9】 両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項 1 ～ 6 の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第 1 のエンティティから第 2 のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項 10】 コンピュータに、平文から積和型の暗号文を得させるためのプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる k 個の成分を有する平文ベクトル、 n 個の任意の乱数を成分とする疑似平文ベクトル、及び、前記 k 個の成分または前記 n 個の成分の位置を特定する情報を示す h 個の成分を有する位置特定ベクトルを加えた $K (= k + n + h)$ 個の成分を有する伸長平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、得られた前記伸長平文ベクトルと公開された公開鍵ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型暗号に関する。

【 0 0 0 2 】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【 0 0 0 3 】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【 0 0 0 4 】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を平文に復号す

る。

【0005】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

公開鍵暗号系の1つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文を K 分割した平文ベクトル $m = (m_1, m_2, \dots, m_K)$ と公開鍵である基数ベクトル $c = (c_1, c_2, \dots, c_K)$ とを用いて、暗号文 $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$ を作成し、受信者である他方のエンティティ側でその暗号文 C を秘密鍵を用いて平文ベクトル m に復号して元の平文を得る暗号化方式である。

【0007】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剰余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000-89669号）。この暗号化方法は、基数ベクトル c の成分 c_i （ $i = 1, 2, \dots, K$ ）を、互いに素な K 個の整数 d_i を用いて $D_i = d / d_i$ （但し、 $d = d_1 d_2 \dots d_K$ ）に設定した基数 D_i を基にモジュラ変換したもの、または、互いに素な K 個の整数 d_i 、乱数 v_i を用いて $D_i = (d / d_i) v_i$ に設定した基数 D_i を基にモジュラ変換したものにすることを特徴としている。このようにして、中国人の剰余定理を用いて並列に復号するので、高速な復号を行うことができる。

【0008】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、LLL (Lenstra-Lenstra-Lovasz) アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【0009】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信方法及び暗号通信システム、並びに、この暗号化方法の動作プログラムを記録した記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】

請求項1に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなる k 個の成分を有する第1ベクトル、 n 個の任意の乱数を成分とする第2ベクトル、及び、前記 k 個の成分または前記 n 個の成分の位置を特定する情報を示す h 個の成分を有する第3ベクトルを加えた $K (= k + n + h)$ 個の成分を有する第4ベクトルと、公開されている第5ベクトルとを用いて暗号文を得ることを特徴とする。

【0011】

請求項2に係る暗号化方法は、請求項1において、前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第4ベクトルにおける前記 h 個の成分の位置は同一であることを特徴とする。

【0012】

請求項3に係る暗号化方法は、請求項1において、前記暗号文は、前記第4ベクトルと前記第5ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記 k 個の成分に応じて次のブロックでの前記第4ベクトルにおける前記 k 個の成分または前記 n 個の成分の位置を決定することを特徴とする。

【0013】

請求項 4 に係る暗号化方法は、請求項 1 において、前記暗号文は、前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる 1 つのブロックと、前記第 3 ベクトルの h 個の成分を平文を分割してなる h 個の成分に置き換えた前記第 4 ベクトルと前記第 5 ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記 k 個または $(k + h)$ 個の成分に応じて次のブロックでの前記第 4 ベクトルにおける $(k + h)$ 個の成分または前記 n 個の成分の位置を決定することを特徴とする。

【 0 0 1 4 】

請求項 5 に係る暗号化方法は、請求項 1 ～ 4 の何れかにおいて、前記第 5 ベクトルは、1 または複数組の整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて各組毎に K 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_K$ (任意の 2 つの整数 d_i, d_j は互いに素)) に設定された 1 または複数の第 6 ベクトルとを用いて生成することを特徴とする。

【 0 0 1 5 】

請求項 6 に係る暗号化方法は、請求項 5 において、前記第 4 ベクトルの各成分と、前記第 6 ベクトルを基にモジュラ変換した前記第 5 ベクトルの各成分とによる積和演算により暗号文を得るようにしたことを特徴とする。

【 0 0 1 6 】

請求項 7 に係る復号方法は、請求項 1 ～ 6 の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記第 1 ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする。

【 0 0 1 7 】

請求項 8 に係る暗号通信方法は、第 1 のエンティティ側で、請求項 1 ～ 6 の何れかに記載の暗号化方法に従って平文から暗号文を作成して第 2 のエンティティ側へ伝送し、伝送された暗号文を該第 2 のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、平文を分割してなる前記 k 個もしくは $(k + h)$ 個の成分または前記 n 個の成分の位置を前記一方のエンティティ側で任意に決定することを特徴とする。

【 0 0 1 8 】

請求項9に係る暗号通信システムは、両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1～6の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第1のエンティティから第2のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする。

【0019】

請求項10に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなる k 個の成分を有する平文ベクトル、 n 個の任意の乱数を成分とする疑似平文ベクトル、及び、前記 k 個の成分または前記 n 個の成分の位置を特定する情報を示す h 個の成分を有する位置特定ベクトルを加えた $K (= k + n + h)$ 個の成分を有する伸長平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、得られた前記伸長平文ベクトルと公開された公開鍵ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする。

【0020】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文を作成する。即ち、暗号化すべき平文を分割してなる第1ベクトル（平文ベクトル）、特に暗号化を必要としない乱数成分からなる第2ベクトル（疑似平文ベクトル）、及び、第1ベクトルまたは第2ベクトルの各成分の位置を示す第3ベクトル（位置特定ベクトル）を合わせた第4ベクトル（伸長平文ベクトル）と、公開されている第5ベクトル（公開鍵ベクトル）とを用いて暗号文を作成する。具体的には、第4ベクトル（伸長平文ベクトル）の各成分と、1または複数の第6ベクトル（基数ベクトル）を基にモジュラ変換した第5ベクトル（公開鍵ベクトル）の各成分との積和演算によって暗号文を構成する。この際、第1ベクトルまたは第2ベクトルの各成分の位置は、暗号文を作成する送信側のエンティティで決定する。また、第3ベクトルの各成分の位置は公開とする。

【0021】

本発明では、暗号化が必要でない冗長部分（退化部分）を付加しているため、暗号文の密度が高くなり、また、1つの第1ベクトル（平文ベクトル）に対して非常に多数の第4ベクトル（平文ベクトル）つまり非常に多数の暗号文が存在するので、LLLアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。また、本来の暗号化すべき平文部分である第1ベクトル（平文ベクトル）の各成分の位置、または、冗長部分（退化部分）である第2ベクトル（疑似平文ベクトル）の各成分を付加する位置は、固定でなく、送信側のエンティティが任意に決定できる。この位置情報は第3ベクトル（位置特定ベクトル）として暗号文に盛り込まれて、受信側のエンティティへ伝送され、その第3ベクトルの各成分の位置は公開されているので、受信側のエンティティにて、第3ベクトルの成分が復号され、その復号結果に基づき第1ベクトル（平文ベクトル）の各成分の位置が分かって、平文に復号できる。本発明では、このように平文部分の位置または冗長部分（退化部分）の付加位置が固定でなく、送信側のエンティティにて決定するため、その位置が攻撃者には未知であるため、安全性は向上する。

【0022】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

まず、本発明の説明に用いる幾つかの定義について説明する。本発明にあっては、暗号化すべき平文は幾つかの分割平文に分けられる。各分割平文をメッセージベクトル m として扱う。以下に定義する伸長変換によって、メッセージベクトル m はベクトル m' に伸長される。このベクトル m' を、伸長メッセージベクトルと称する。これらのベクトル m 、ベクトル m' の各成分のビットサイズの和を夫々 ε （ビット）、 ε' （ビット）（但し、 $\varepsilon \leq \varepsilon'$ ）とする。また、暗号文が取り得る最大ビット数を C_{\max} とする。

【0023】

〈定義1（密度）〉

方式密度 ρ を下記（1）のように定義する。

【0024】

【数 1】

$$\rho = \frac{\varepsilon'}{\log_2 C_{\max}} \quad \dots (1)$$

【0025】

<定義 2 (レート)>

レート η を下記 (2) のように定義する。

【0026】

【数 2】

$$\eta = \frac{\varepsilon}{|C_{\max}|} \quad \dots (2)$$

【0027】

ベクトル $a = (a_1, a_2, \dots, a_w)$ を w 次元ベクトルとし、ベクトル $c = (c_1, c_2, \dots, c_n)$ を n 次元ベクトルとする。また、ベクトル $b = (b_1, b_2, \dots, b_n)$ を重み w の n 次元 2 値ベクトルとする。但し、下記 (3) の条件を満たす。

【0028】

【数 3】

$$\left. \begin{array}{l} b_{i_1} = b_{i_2} = \dots = b_{i_w} = 1 \\ i_1 < i_2 < \dots < i_w \end{array} \right\} \dots (3)$$

【0029】

<定義 3 (添数集合)>

添数集合 $I = \text{Ind}(\text{ベクトル } b)$ を下記 (4) のように定義する。

$$I = \{i_1, i_2, \dots, i_w\} \quad \dots (4)$$

【0030】

〈定義4 (ベクトル表現)〉

添数集合 I は、 $\{1, 2, \dots, n\}$ の部分集合であり、ベクトル表現として、ベクトル $d = \text{Vec}(I, n)$ を下記(5)のように定義する。但し、ベクトル $d = (d_1, d_2, \dots, d_n)$ であり、例えば、 $I = \text{Ind}(b)$ (ベクトル b) である場合に、ベクトル $b = \text{Vec}(I, n)$ である。

【0031】

【数4】

$$d_i = \begin{cases} 1 & (i \in I) \\ 0 & (i \notin I) \end{cases} \dots (5)$$

【0032】

〈定義5 (伸長)〉

ベクトル b によりベクトル a から伸長された n 次元ベクトル c は、ベクトル $c = \text{ベクトル } a \{ \text{ベクトル } b \}$ にて表記し、下記(6)のように定義する。例えば、ベクトル $a = (a_1, a_2, a_3)$ 、ベクトル $b = (1, 0, 1, 1)$ である場合に、ベクトル $a \{ \text{ベクトル } b \} = (a_1, 0, a_2, a_3)$ となる。

【0033】

【数5】

$$\begin{cases} c_{i_j} = a_j \\ c_k = 0 \end{cases} \dots (6) \quad (b_k = 0 \text{ の場合})$$

$$(j = 1, 2, \dots, w, k = 1, 2, \dots, n)$$

【0034】

〈定義6 (抜き出し)〉

ベクトル b によりベクトル c から抜き出された w 次元ベクトル a は、ベクトル

$a = \text{ベクトル } c \{ \text{ベクトル } b \}$ にて表記し、下記 (7) のように定義する。例えば、ベクトル $c = (c_1, c_2, c_3, c_4)$ 、ベクトル $b = (1, 0, 1, 1)$ である場合に、第1, 第3及び第4成分が抜き出されて、ベクトル $c \{ \text{ベクトル } b \} = (c_1, c_3, c_4)$ となる。

【0035】

【数6】

$$\vec{a} = (c_{i_1}, c_{i_2}, \dots, c_{i_w}) \dots (7)$$

【0036】

次に、本発明の具体的な方式について説明する。

図1は、本発明による暗号化方法をエンティティ a, b間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティ a が、暗号化器1にて平文 x を暗号文 C に暗号化し、通信路3を介してその暗号文 C を他方のエンティティ b へ送信し、エンティティ b が、復号器2にてその暗号文 C を元の平文 x に復号する場合を示している。

【0037】

<平文分割>

平文 x は、 e k ビットの複数のブロックに分割される。各ブロックは下記 (8) のようにメッセージベクトル m で表現される。なお、 m_i ($i = 1, 2, \dots, k$) は e ビットの整数である。

$$\text{ベクトル } m = (m_1, m_2, \dots, m_k) \dots (8)$$

【0038】

<伸長変換>

メッセージベクトル m を、各成分が e ビットの整数である k 次元ベクトルとし、乱数ベクトル r を、各成分が e' ビットの整数である n 次元ベクトルとする。但し、 $e < e'$ とする。また、ベクトル s を、重み k の $(k+n)$ 次元の2値ベクトルとする。このベクトル s を「位置特定子」と称する。

【0039】

h を下記 (9) のように設定し、ベクトル s' を $(he - (k+n))$ ビットの任意の 2 値詰め物ベクトルとする。 he 次元の 2 値連接ベクトル [ベクトル s | ベクトル s'] は、各成分が e ビットの整数である下記 (10) のような h 次元のベクトル t に分割できる。

【0040】

【数 7】

$$h = \lceil (k+n)/e \rceil \quad \dots (9)$$

$$\vec{t} = (t_1, t_2, \dots, t_h) \quad \dots (10)$$

【0041】

$K = k+n+h$ とし、各添数集合 I_N , I_R 及び I_L を夫々下記 (11), (12) 及び (13) のように定義する。但し、バーベクトル \overline{s} はベクトル s のビット補数を表す。

【0042】

【数 8】

$$I_N = \text{Ind}(\vec{s}) \quad \dots (11)$$

$$I_R = \text{Ind}(\overline{\vec{s}}) \quad \dots (12)$$

$$I_L = \{k+n+1, k+n+2, \dots, K\} \quad \dots (13)$$

【0043】

なお、上記例では添数集合 I_L の成分を最後尾の h 個としたが、これらの成分の位置は任意であって良い。このような場合、下記 (14), (15) の条件を満たし、ベクトル m' , ベクトル s は夫々下記 (16), (17) のように表される。

【0044】

【数 9】

$$I_N \cup I_R \cup I_L = \{1, 2, \dots, K\} \quad \dots (14)$$

$$I_N \cap I_R = I_R \cap I_L = I_L \cap I_N = \phi \quad \dots (15)$$

$$\begin{aligned} \vec{m}' &= \vec{m} \{Vec(I_N, K)\} + \\ &\quad \vec{r} \{Vec(I_R, K)\} + \vec{t} \{Vec(I_L, K)\} \quad \dots (16) \end{aligned}$$

$$\vec{s} = Vec(I_N, K) [\overline{Vec(I_L, K)}] \quad \dots (17)$$

【0045】

メッセージベクトル m を、下記 (18) のように、伸長メッセージベクトル $m' = (m_1', m_2', \dots, m_K')$ に変換する。この際、このベクトル m' の各成分の大きさは下記 (19) である。

【0046】

【数 10】

$$\vec{m}' = [\vec{m} \{ \vec{s} \} + \vec{r} \{ \vec{s} \} | \vec{t}] \quad \dots (18)$$

$$|m_i'| = \begin{cases} e & (i \in I_N \cup I_L) \\ e' & (i \in I_R) \end{cases} \quad \dots (19)$$

【0047】

<鍵生成>

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵： $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$, $\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$,

P , Q , N , w (但し、 $i = 1, 2, \dots, K$)

・公開鍵：ベクトル $c = (c_1, c_2, \dots, c_K)$, I_L , e , e'

なお、上記 N は公開であっても良い。

【0048】

まず、任意の i, j (但し、 $i \neq j$) について、下記 (20) ~ (23) の条件を満たすような2組の基数 $\{d_i^{(P)}\}, \{d_i^{(Q)}\}$ を生成する。

【0049】

【数11】

$$\gcd(d_i^{(P)}, d_j^{(P)}) = 1 \quad \dots (20)$$

$$\gcd(d_i^{(Q)}, d_j^{(Q)}) = 1 \quad \dots (21)$$

$$\gcd(d_i^{(P)}, d_j^{(Q)}) = 1 \quad \dots (22)$$

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \dots (23)$$

【0050】

$v_i^{(P)}, v_i^{(Q)}$ をランダムな整数として、下記 (24), (25) のように、 $V_i^{(P)}, V_i^{(Q)}$ を導く。但し、 $v_i^{(P)}$ 及び $v_i^{(Q)}$ は、下記 (26) 及び (27) の条件を満たす。

【0051】

【数12】

$$V_i^{(P)} = \frac{d_1^{(P)} d_2^{(P)} \dots d_k^{(P)}}{d_i^{(P)}} v_i^{(P)} \quad \dots (24)$$

$$V_i^{(Q)} = \frac{d_1^{(Q)} d_2^{(Q)} \dots d_k^{(Q)}}{d_i^{(Q)}} v_i^{(Q)} \quad \dots (25)$$

$$\gcd(d_i^{(P)}, v_i^{(P)}) = 1 \quad \dots (26)$$

$$\gcd(d_i^{(Q)}, v_i^{(Q)}) = 1 \quad \dots (27)$$

【0052】

次に、任意の伸長メッセージベクトル m' について条件 $M_P < P, M_Q < Q$ を満たすような大きな素数 P, Q を設定する。なお、 M_P, M_Q は夫々下記 (28), (29) で定義される。

【0053】

【数13】

$$M_P = m'_1 V_1^{(P)} + m'_2 V_2^{(P)} + \dots + m'_K V_K^{(P)} \dots (28)$$

$$M_Q = m'_1 V_1^{(Q)} + m'_2 V_2^{(Q)} + \dots + m'_K V_K^{(Q)} \dots (29)$$

【0054】

そして、 $N=PQ$ を設定し、中国人の剰余定理により V_i ($0 \leq V_i < N$)を下記(30)により計算する。

【0055】

【数14】

$$V_i \equiv \begin{cases} V_i^{(P)} \pmod{P} \\ V_i^{(Q)} \pmod{Q} \end{cases} \dots (30)$$

【0056】

公開鍵ベクトル c の各成分を、下記(31)により求める。ここで w は、 Z_N^* から任意に選ばれた乱数である。

$$c_i \equiv w V_i \pmod{N} \dots (31)$$

【0057】

〈暗号化〉

エンティティ a 側(送信側)で、前述した位置特定子であるベクトル s を任意に生成する。即ち、メッセージベクトル m に関する位置を示す添数集合 I_N を、送信者であるエンティティ a は任意に選択する。次に、エンティティ a 側(送信側)で、各成分が任意に選択された e' ビットの整数からなる n 次元のベクトル r を生成する。この乱数ベクトル r により、高密度が実現される。つまり、冗長部分(退化部分)である乱数ベクトル r の付加によって、後述するように密度が高くなる。

【0058】

エンティティ a 側（送信側）で、メッセージベクトル m を、ベクトル s 及びベクトル r によって、伸長メッセージベクトル m' に変換する。そして、この伸長メッセージベクトル m' と公開鍵ベクトル c との内積を下記 (32) のように求めて、暗号文 C を得る。作成された暗号文 C は通信路 3 を介してエンティティ a からエンティティ b へ送信される。

【0059】

【数15】

$$\begin{aligned} C &= \vec{m'} \cdot \vec{c} \\ &= m'_1 c_1 + m'_2 c_2 + \dots + m'_K c_K \quad \dots \quad (32) \end{aligned}$$

【0060】

この暗号化にあつては、暗号化すべき平文を分割したメッセージベクトル m は、添数集合 I_N にて示される位置で伝送され、添数集合 I_N の情報は、添数集合 I_L にて示される位置でベクトル s によって伝送される。

【0061】

<復号>

エンティティ b 側（受信側）で、以下のようにして復号処理が行われる。

中間メッセージ M は、下記 (33) を満たす。従つて、法 P 、法 Q における中間メッセージ M_P 、 M_Q は、下記 (34)、(35) のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \dots (33)$$

$$M_P \equiv M \pmod{P} \quad \dots (34)$$

$$M_Q \equiv M \pmod{Q} \quad \dots (35)$$

【0062】

そして、下記 (36)、(37) によって $(m_i^{(P)}, m_i^{(Q)})$ を求め、中国人の剰余定理を適用することにより、下記 (38) が成立して、メッセージベクトル $m'' = (m_1'', m_2'', \dots, m_K'')$ を復号することができる。

【0063】

【数16】

$$m_i^{(P)} \equiv M_P V_i^{(P)^{-1}} \pmod{d_i^{(P)}} \dots (36)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)^{-1}} \pmod{d_i^{(Q)}} \dots (37)$$

$$m_i'' \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \dots (38)$$

【0064】

$e' > e$ であるので、復号されたメッセージベクトル m'' の各成分は、上記(19)から、下記(39)の条件を満たす。

【0065】

【数17】

$$\begin{cases} m_i'' = m_i' & (i \in I_N \cup I_L) \\ m_i'' \neq m_i' & (i \in I_R) \end{cases} \dots (39)$$

【0066】

添数集合 I_L に従って、下記(40)のように、復号ベクトル m'' からベクトル t を取り出す。

【0067】

【数18】

$$\vec{t} = \vec{m}'' [\text{Vec}(I_L, K)] \dots (40)$$

【0068】

ベクトル t を $h \times e$ 次元の2値ベクトル[ベクトル s | ベクトル s']と見なすことにより、 $(k+n)$ 次元で重み k の2値ベクトル s をエンティティ b 側(受信側)で再構築できる。よって、最終的に、下記(41)のように、メッセージベクトル m を得ることができる。

【0069】

【数19】

$$\vec{m} = \vec{m}'' [\vec{s}] \quad \cdots (41)$$

【0070】

なお、添数集合 I_L の成分を任意とする一般的な場合には、上記 (41) において、ベクトル m'' を下記 (42) に示すものに代えることにより、メッセージベクトル m が得られる。

【0071】

【数20】

$$\vec{m}'' [\overline{\text{Vec}(I_L, K)}] \quad \cdots (42)$$

【0072】

次に、上述したような本発明の暗号化方式における安全性について述べる。密度が0.9408より小さい場合には、本発明のような積和型公開鍵暗号はLLLアルゴリズムに基づく低密度攻撃によって破られることが知られている。上述した本発明の暗号化方式では、1を超える高い密度を実現できており、このことはこの方式が低密度攻撃に対して安全であることを示している。

【0073】

乱数 $v_i^{(P)}$, $v_i^{(Q)}$ を何れも f ビットとした場合、上述した本発明の暗号化方式における密度 ρ は、下記 (43) の条件を満たす。但し、 $K = k + n + h$, $e' > e$ である。

【0074】

【数21】

$$\begin{aligned} \rho &> \frac{(k+h) e + n e'}{e' + \log_2 N + \log_2 n} \\ &> \frac{K e + n (e' - e)}{K e + (3 e' - e) + f + 1 + 3 \log_2 n} \quad \cdots (43) \end{aligned}$$

【0075】

例えば、ここで簡単のために、 $f = e$ 、 $e' = 2e$ と設定した場合、 n は下記(44)の条件を満たすので、 $\rho > 1$ を実現できている。現実的な例として、 $e = 32$ とした場合、何れの k についても $n = 7$ とすることにより、 $\rho > 1$ を達成できることが分かる。

【0076】

【数22】

$$(n-6)e > 3 \log_2 n + 1 \quad \dots (44)$$

【0077】

また、本発明の暗号化方式では、高いレートも実現できている。上述した本発明の暗号化方式におけるレート η は、下記(45)の条件を満たす。

【0078】

【数23】

$$\begin{aligned} \eta &= \frac{ke}{\lceil e' + \log_2 N + \log_2 n \rceil} \\ &> \frac{ke}{Ke + (3e' - e) + f + 1 + 3 \log_2 n} \quad \dots (45) \end{aligned}$$

【0079】

ここで簡単のために、 $f = e$ 、 $e' = 2e$ と設定した場合、 n 及び k は下記(46)の条件を満たすので、 $\eta > 0.5$ を実現できている。現実的な例として、 $e = 32$ とした場合、 $n = 7$ で $k > 14$ とすることにより、 $\eta > 0.5$ を達成できることが分かる。例えば、 $k = 57$ とした場合に、 $\eta \doteq 0.7884$ となる。このように、レートの観点から見ても、本発明の方式は効率的である。

【0080】

【数 24】

$$\left(k - n - \left\lceil \frac{k+n}{e} \right\rceil - 6\right)e > 3 \log_2 n + 1 \quad \cdots (46)$$

【0081】

本発明の暗号化方式では、高い密度を実現できるため、低密度攻撃に対し、十分に安全である。また、送信側のエンティティにおいて、退化基数の位置を自由に決定できる。よって、位置が分かっている退化基数に基づき、攻撃者が本発明の暗号化方式に対して有効な攻撃を行おうとした場合でも、その攻撃者にとって退化基数の位置を同定することが困難である。従って、退化基数の位置が固定ではなく送信側で任意に決定できるという本発明の特徴は、退化基数の位置が既知である場合に有効である攻撃に対しても安全であることを示している。

【0082】

以下、本発明の他の実施の形態について説明する。上述した例では全てのブロックにおいて、 I_L の位置を固定（最後尾）としているが、この I_L の位置は各ブロックにおいて異なっても良い。このような例として、以下のようなものが可能である。

【0083】

(第1例)

最初のブロックについては I_L の位置を固定（例えば上述した例と同様に最後尾）し、この I_L は公開しておく。そして、2番目以降のブロックについては、1つ前のブロックのメッセージベクトルよりそのブロックの I_L の位置を決定するようにする。よって、2番目以降のブロックからは、 I_L の位置が変動する。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックの I_L は公開されており、しかも、2番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックの I_L の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。この第1例では、各ブロックにおいて I_L の位置を変動させるため、安全性

の向上を図れる。

【0084】

(第2例)

最初のブロックについては I_L の位置を固定 (例えば上述した例と同様に最後尾) し、この I_L は公開しておく。そして、2番目以降のブロックについては、 I_L の項を設けないようにし、 I_L の項に割り当てられる h 次元のベクトルを平文を分割したメッセージに割り当てる。そして、この2番目以降のブロックについては、1つ前のブロックのメッセージよりそのブロックにおける退化基数の位置を示す位置情報を決定する。よって、2番目以降のブロックには、 I_L が存在しない。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックの I_L は公開されており、しかも、2番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックでの退化基数の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。また、2番目以降のブロックではメッセージに割り当てる部分が k 項から $(k+h)$ 項に増えるので、1ブロック内に盛り込めるメッセージ量が増加して、レートをより高くすることができる。

【0085】

なお、上記例では、暗号化すべき平文を分割したメッセージベクトル m の各成分の位置 (添数集合 I_N) を示す情報 (添数集合 I_L) を伝送するようにしたが、付加する乱数ベクトル r の各成分の位置 (添数集合 I_R) を示す情報を伝送するようにしても良いことは勿論である。

【0086】

また、上記例では、2組の基数 $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$ に乱数 $\{v_i^{(P)}\}$, $\{v_i^{(Q)}\}$ を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【0087】

また、上記例では、 K 個の要素からなる基数の集合 $\{d_i\}$ を2組 ($\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$) 生成する多重化した方式の場合について説明したが、1組の基数の集合 $\{d_i\}$ を用いる方式についても、本発明を同様に適用できること

は勿論である。

【0088】

図2は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した暗号化方式の手順に従って伸長平文ベクトル m' を得る処理と、得た伸長平文ベクトル m' と公開鍵ベクトル c との内積計算により暗号文 C を作成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【0089】

図2において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11aが記録されている。記録媒体11から通信線等の伝送媒体14を介して読み出されたプログラム11aがコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0090】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体12には前述の如きプログラム12aが記録されている。記録媒体12から読み出されたプログラム12aがコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0091】

コンピュータ10に設けられたディスクドライブ10aに装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13aが記録されている。記録媒体13から読み出されたプログラム13aがコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0092】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる第1ベクトル（

平文ベクトル)、特に暗号化を必要としない乱数成分からなる第2ベクトル(疑似平文ベクトル)、及び、第1ベクトルまたは第2ベクトルの各成分の位置を示す第3ベクトル(位置特定ベクトル)を合わせた第4ベクトル(伸長平文ベクトル)と、公開されている第5ベクトル(公開鍵ベクトル)とを用いて暗号文を作成する。具体的には、第4ベクトル(伸長平文ベクトル)の各成分と、1または複数の第6ベクトル(基数ベクトル)を基にモジュラ変換した第5ベクトル(公開鍵ベクトル)の各成分との積和演算によって暗号文を構成し、第1ベクトルまたは第2ベクトルの各成分の位置を、暗号文を作成する送信側のエンティティで決定するようにしたので、暗号化が必要でない冗長部分(退化部分)を付加しているため、暗号文の密度を大きくでき、LLLアルゴリズムに基づく低密度攻撃に対して強くなって安全性を向上でき、また、暗号化すべき平文部分の位置または冗長部分(退化部分)の付加位置は、固定でなく、送信側のエンティティが任意に決定できるため、攻撃者にとってその位置を見つけることすら困難であり、安全性の更なる向上を図れる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図1】

2人のエンティティ間における情報の通信状態を示す模式図である。

【図2】

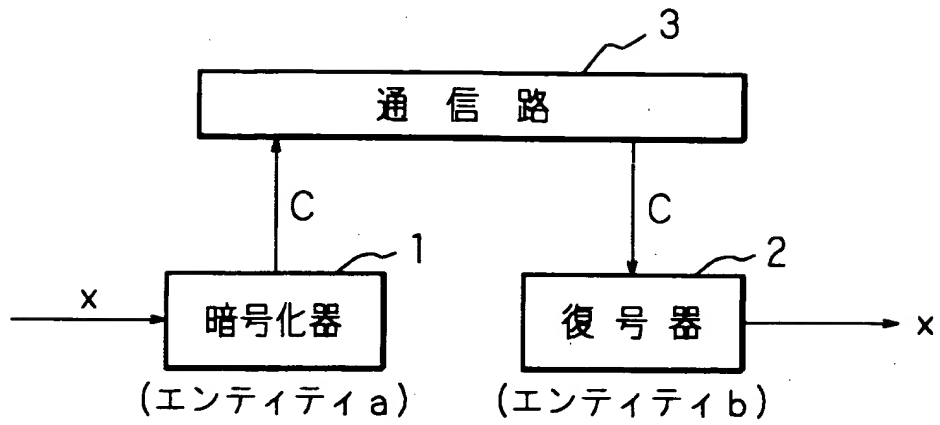
記録媒体の実施の形態の構成を示す図である。

【符号の説明】

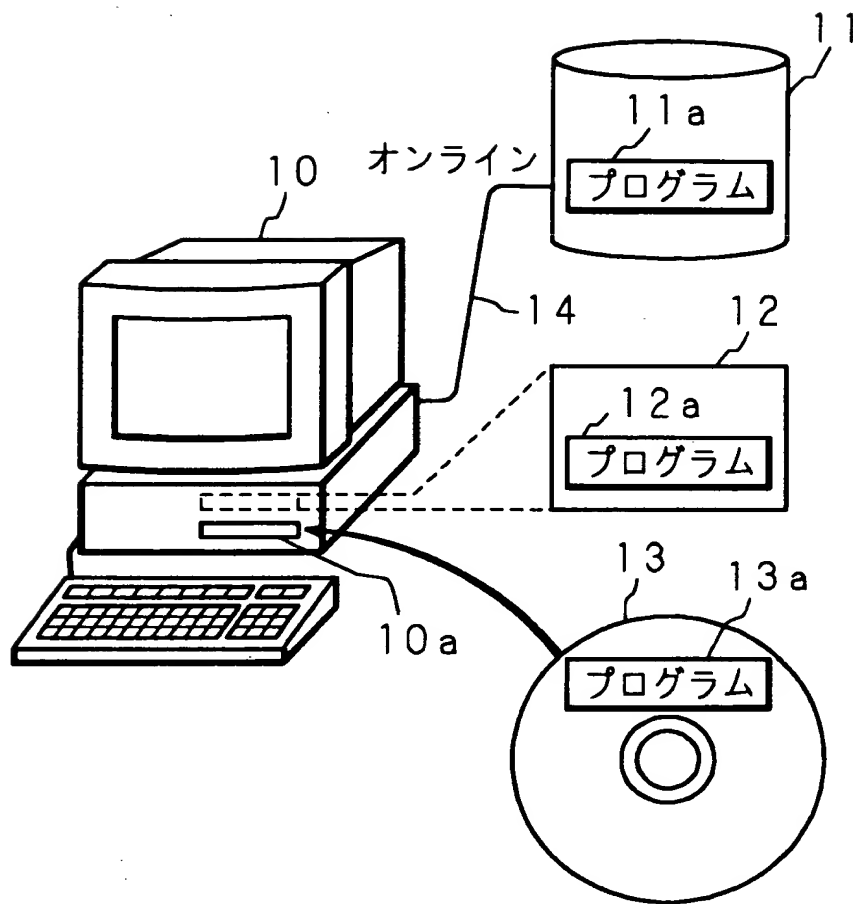
- 1 暗号化器
- 2 復号器
- 3 通信路
- a, b エンティティ

【書類名】 図面

【図 1】



【図2】



【書類名】 要約書

【要約】

【課題】 LLLアルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方式を提供する。

【解決手段】 暗号化すべき平文を分割した平文ベクトル、任意の乱数成分からなる疑似平文ベクトル、及び、平文ベクトルまたは疑似平文ベクトルの成分の位置を特定する情報を有する位置情報ベクトルを加えた伸長平文ベクトルの各成分と、1または複数組の整数 d_i ($1 \leq i \leq K$) 及び乱数 v_i を用いて $V_i = (d/d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_K$ (任意の2つの整数 d_i, d_j は互いに素)) に設定された1または複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得る。平文ベクトルまたは疑似平文ベクトルの成分の位置は、送信側(エンティティ a)が決定する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地
氏 名 村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日 1997年 1月21日

[変更理由] 新規登録

住 所 大阪府箕面市栗生外院4丁目15番3号

氏 名 笠原 正雄